APPENDIX: Clean copy of the claims after amendment

1. (Currently amended) A method comprising:

a central management entity managing managed access points (APs) of a wireless network, including carrying out one or both of power control and frequency selection to configure one or more configuration parameters of the managed access point;

maintaining an AP database that includes information about managed APs and friendly APs of the wireless network, including for each managed AP in the AP database, the service set identifier of the managed AP and one or more of the configuration parameters;

sending a scan request to one or more managed APs of the wireless network, the scan request including a request for the receiving managed AP to scan for beacons and probe responses; and

receiving reports from at least one of the receiving managed APs about beacons or probe responses from any potential rogue AP, including, for each potential rogue AP from which a beacon or probe response was received, detection information, and information on the beacon or probe response received sent by the potential rogue AP,

wherein the detection information includes the service set identifier of the potential rogue AP, and at least one further item of information, and

wherein the information on the received beacon or probe response includes at least the service set identifier in the beacon or probe response, and one or more configuration parameters; and

for each beacon or probe response from a potential rogue AP on which information is received, ascertaining if the potential rogue AP is a managed AP, including:

ascertaining if there is a match for the service set identifier of the potential rogue AP in the AP database, and if there is a match for one or more configuration parameters of the potential rogue AP in the AP database in addition to the service set identifier of the potential rogue AP,

such that at least a plurality of parameters are matched in the AP database to ascertain whether a potential rogue AP is a managed AP.

2. (Original) A method as recited in claim 1, wherein the wireless network substantially conforms to the IEEE 802.11 standard for wireless local area networks.

3. (Original) A method as recited in claim 1, wherein the maintaining the AP database includes updating the AP database from time to time.

4. (Cancelled).

5. (Previously presented) A method as recited in claim 1, wherein the analysis further includes determining the approximate location of the potential rogue AP in order to further ascertain whether the potential rogue AP is likely to be a rogue, a location determining method that uses information determined from signals received from the potential rogue AP at a plurality of managed APs whose locations are known or at stations whose respective locations are known or determined, and calculating a likely location using the determined information.

6. (Previously presented) A method as recited in claim 1, wherein the sending a request includes sending a request to one or more wireless stations of the wireless network to listen for beacons and probe responses on the respective serving channels of the respective wireless stations and to report the results of the listening.

7. (Previously presented) A method as recited in claim 1, wherein the sending a request includes sending a request for one or more wireless stations to temporarily listen for

beacons and probe responses on a channel specified in the request and to report the results of the listening.

8. (Original) A method as recited in claim 1, wherein the sending a request includes sending a request for one or more managed access points to listen for beacons and probe responses and to report the results of the listening.

9. (Original) A method as recited in claim 1, wherein the sending a request includes sending a request for one or more clients of one or more managed access points to listen for beacons and probe responses and to report the results of the listening.

10. (Cancelled).

11. (Previously presented) A method as recited in claim 1, wherein the analyzing further includes using timing information determined from the beacon or probe response to further ascertain whether the AP is likely to be a rogue.

12. (Original) A method as recited in claim 11, wherein the analyzing further includes using known location information of managed APs together with the timing information to determine the approximate location of the potential rogue AP.

13. (Currently amended) A method as recited in claim 1, wherein the detection information includes absolute RSSI information, and wherein the analyzing further includes using known location information of managed APs to approximately locate the potential rogue AP, and method further comprising:

> locating the potential rogue AP by using the absolute RSSI at the station receiving the beacon or probe response together with a calibrated path loss model of an area of interest that provides path losses at various locations to or from managed stations at known locations.

14. (Original) A method as recited in claim 13, wherein the locating includes:

accepting an ideal path loss model applicable to an area of interest;

calibrating the ideal path loss model using measurements received from each respective managed station of a first set of managed wireless stations of the wireless network measuring the received signal strengths at each of the respective managed stations, the managed stations receiving signals as a result of transmissions by respective managed stations of a second set of managed wireless stations of the wireless network, each respective transmission at a known respective transmit power, the locations of each managed station of the first and second set being known or determined, the calibrating being to determine a calibrated path loss model between the receiving and transmitting wireless stations;

receiving measurements from each respective managed station of a third set of managed wireless stations of the wireless network measuring the received signal strength at each of the respective stations resulting from transmission of a beacon or probe response from a potential rogue access point, each station of the third set being at a known or determined location; and

for each of a set of assumed transmit powers for the potential rogue access point, determining the likely location or locations of the potential rogue access point using the received signal strengths at the stations of the third set and the calibrated path loss model.

15. (Original) A method as recited in claim 14, wherein the determining of the likely location or locations includes:

determining a set of likelihood components for each of a set of locations, each component corresponding to a respective managed access point whose transmissions are listened for at the particular station, and

determining an overall likelihood for each of the set of locations as the product of the likelihood components.

16. (Original) A method as recited in claim 1, wherein further comprising combining the results of the analyzing step with the results of one or more complementary rogue AP detection techniques.

17. (Original) A method as recited in claim 16, wherein one of the complementary rogue AP detection techniques includes a client reporting to a managed AP a failed previous authentication attempt with an AP.

18. (Currently amended) A method comprising:

receiving a scan request at an access point (AP) of a wireless network to scan for beacons and probe responses, the request received from a management entity coupled to a WLAN manager managing a set of managed APs, the managing of the managed APs including carrying out one or both of power control and frequency selection to configure one or more configuration parameters of the managed APs and maintaining an AP database that contains information about managed APs and friendly APs of the wireless network, the information in the AP database including for each managed AP in the AP database, the service set identifier of the managed AP and one or more of the configuration parameters;

listening for beacons and probe responses at the AP receiving the scan; and

sending a scan report to the WLAN manager including information on any beacon or probe response received from a potential rogue AP by the AP receiving the scan request, the information including, for each potential rogue AP from which a beacon or probe response was received, detection information, and information on the beacon or probe response from the potential rogue AP,

wherein the detection information includes the service set identifier of the potential rogue AP, and at least one further item of information, and

wherein the information on the received beacon or probe response includes at least the service set identifier in the beacon or probe response, and one or more configuration parameters,

such that for each beacon or probe response from a potential rogue AP on which information is received at the WLAN manager, ascertaining if the potential rogue AP is a managed AP, including:

ascertaining if there is a match for the service set identifier of the potential rogue AP in the AP database, and if there is a match for one or more configuration parameters of the potential rogue AP in the AP database in addition to the service set identifier of the potential rogue AP,

such that at least a plurality of parameters are matched in the AP database to ascertain whether a potential rogue AP is a managed AP.

19. (Original) A method as recited in claim 18, wherein the scan request includes a request to scan for beacons and probe responses on the respective serving channel of each respective wireless AP or client station and to report the results of the listening.

20. (Original) A method as recited in claim 18, wherein the scan request a includes a request for the listening stations AP or client station to temporarily listen for beacons and probe responses on a channel specified in the request and to report the results of the listening.

21. (Original) A method as recited in claim 18, wherein the scan request from the WLAN manager and the scan report to the WLAN manager use a protocol that provides for and encapsulates scan request messages and scan report messages in IP packets.

22. (Original) A method as recited in claim 21, wherein the request from an AP to a client station, and the report from the client station to an AP uses MAC frames.

23. (Currently amended) A method as recited in claim 21, wherein the scan request includes a set of scan parameters that describe how information is to be obtained about beacons and probe responses received by the managed.

24. (Currently amended) A method as recited in claim 23, wherein the scan parameters include one or more of:

whether the requested scan is an active scan or a passive scan or both an active and passive scan, and if an active scan, one or more channels for the active scan, and

the schedule of how often scans are to be performed.

25. (Currently amended) A method as recited in claim 23, wherein after receiving the task request, the receiving AP sets up tasking according to the scan request, including scheduling any scans to be performed by the receiving AP.

26. (Currently amended) A computer-readable medium encoded with computer readable instructions that when executed cause one or more processors of a processing system to execute a method comprising:

managing managed access points (APs) of a wireless network, including carrying out one or both of power control and frequency selection to configure one or more configuration parameters of each managed access point;

maintaining an AP database that includes information about managed APs and friendly APs of the wireless network, including for each managed AP in the AP databse, the service set identifier of the managed AP and one or more of the configuration parameters;

sending a scan request to one or more managed APs of the wireless network, the scan request including a request for the receiving managed AP to scan for beacons and probe responses; and

receiving reports from at least one of the receiving managed APs about beacons or probe responses from any potential rogue AP, including, for each potential rogue AP from which a beacon or probe response was received, detection information, and information on the beacon or probe response received sent by the potential rogue AP,

wherein the detection information includes the service set identifier of the potential rogue AP, and at least one further item of information, and

wherein the information on the received beacon or probe response includes at least the service set identifier in the beacon or probe response, and one or more configuration parameters; and

for each beacon or probe response from a potential rogue AP on which information is received, ascertaining if the potential rogue AP is a managed AP, including:

ascertaining if there is a match for the service set identifier of the potential rogue AP in the AP database, and if there is a match for one or more configuration parameters of the potential rogue AP in the AP database in addition to the service set identifier of the potential rogue AP,

such that at least a plurality of parameters are matched in the AP database to ascertain whether a potential rogue AP is a managed AP.

27. (Currently amended) A computer-readable medium encoded with computer readable instructions to instruct one or more processors of a processing system to execute a method at an access point (AP) of a wireless network comprising:

receiving a scan request to scan for beacons and probe responses, the request received from a management entity coupled to a WLAN manager managing a set of managed APs, the managing of the managed APs including carrying out one or both of power control and frequency selection to configure one or more configuration parameters of the managed APs and maintaining an AP database that contains information about the managed APs and friendly APs of the wireless network, the

information in the AP database including for each managed AP in the AP database, the service set identifier of the managed AP and one or more of the configuration parameters;

listening for beacons and probe responses at the AP receiving the scan request; and

sending a scan report to the WLAN manager including information on any beacon or probe response received from a potential rogue AP by the AP receiving the scan request, the information including, for each potential rogue AP from which a beacon or probe response was received, detection information, and information on the beacon or probe response from the potential rogue AP,

wherein the detection information includes the service set identifier of the potential rogue AP, and at least one further item of information, and

wherein the information on the received beacon or probe response includes at least the service set identifier in the beacon or probe response, and one or more configuration parameters,

such that for each beacon or probe response from a potential rogue AP on which information is received at the WLAN manager, ascertaining if the potential rogue AP is a managed AP, including:

ascertaining if there is a match for the service set identifier of the potential rogue AP in the AP database, and if there is a match for one or more configuration parameters of the potential rogue AP in the AP database in addition to the service set identifier of the potential rogue AP

such that at least a plurality of parameters are matched in the AP database to ascertain whether a potential rogue AP is a managed AP.

28. (Currently amended) An apparatus comprising:

a processing system including a memory and a network interface to couple the apparatus to a network, the network including a set of managed access points (APs) of a wireless network; and

a tangible medium storing an AP database coupled to the processing system and containing information about the managed APs and friendly APs of the wireless network, including information related to how each managed AP in the AP database is configured,

wherein the processing system is programmed to:

manage the managed APs, including carrying out one or both of power control and frequency selection to configure one or more configuration parameters of each managed access point;

maintain the AP database that includes information about the managed APs, including for each managed AP, the service set identifier of the managed AP and one or more of the configuration parameters;

send a scan request to one or more managed APs of the wireless network, the scan request being for the receiving managed AP to scan for beacons and probe responses; and

receive reports from at least one of the receiving managed APs about beacons or probe responses from any potential rogue AP, including, for each potential rogue AP from which a beacon or probe response was received, detection information, and information on the beacon or probe response received sent by the potential rogue AP,

wherein the detection information includes the service set identifier of the potential rogue AP, and at least one further item of information, and

wherein the information on the received beacon or probe response includes at least the service set identifier in the beacon or probe response, and one or more configuration parameters; and

for each beacon or probe response from a potential rogue AP on which information is received, ascertaining if the potential rogue AP is a managed AP, including:

ascertaining if there is a match for the service set identifier of the potential rogue AP in the AP database, and if there is a match for one or more configuration parameters of the potential rogue AP in the AP database in addition to the service set identifier of the potential rogue AP,

such that at least a plurality of parameters are matched in the AP database to ascertain whether a potential rogue AP is a managed AP.

29. (Currently amended) An access point (AP) for a wireless network, the access point comprising:

a processing system including a memory;

a network interface to couple the access point to a network;

a wireless transceiver coupled to the processing system to implement the PHY of a wireless station;

the processing system including a MAC processor and programmed to:

receive a scan request to scan for beacons and probe responses, the request received via the network interface from a management entity coupled to a WLAN manager coupled to the network and managing a set of managed, the managing including carrying out one or both of power control and frequency selection to configure one or more configuration parameters of managed APs and maintaining an AP database that contains information about managed APs and friendly APs of the wireless network,

including for each managed AP in the AP database, the service set identifier of the managed AP, and one or more of the configuration parameters; and

send a scan report to the WLAN manager via the network interface, including information on any beacon or probe response received from a potential rogue AP, the scan report including for each potential rogue AP beacon or probe response was received, detection information, and information on the beacon or probe response from the potential rogue AP,

wherein the detection information includes the service set identifier of the potential rogue AP, and at least one further item of information, and

wherein the information on the received beacon or probe response includes at least the service set identifier in the beacon or probe response, and one or more configuration parameters,

such that for each beacon or probe response on which information is received at the WLAN manager, analyzing the information received in the report about the potential rogue AP that sent the beacon or probe response includes, in order to ascertain if the potential rogue AP is a managed AP:

(a) ascertaining if there is a match for the service set identifier of the potential rogue AP in the AP database, and

(b) ascertaining if there is a match for one or more configuration parameters of the potential rogue AP in the AP database in addition to the service set identifier of the potential rogue AP,

such that at least a plurality of parameters are matched in the AP database to ascertain whether a potential rogue AP is a managed AP.

30. (New) A method as recited in claim 1, wherein the information stored in the AP database on each managed AP includes a maximum power setting or a frequency setting or both a maximum power and a frequency setting.

31. (New) A method as recited in claim 1, wherein the detection information includes at least the channel the detected AP's beacon or probe response was received on, and wherein the information on the received beacon or probe response includes at least a service set identifier in the beacon or probe response.

32. (New) A method as recited in claim 1, wherein the sending a scan request to one or more managed APs of the wireless network includes a request for the receiving managed AP to request the AP's clients to scan for beacons and probe responses.

33. (New) A method as recited in claim 18, wherein the information stored in the AP database on each managed AP includes a maximum power setting or a frequency setting or both a maximum power and a frequency setting.

34. (New) A method as recited in claim 18, wherein the detection information includes at least the channel the detected AP's beacon or probe response was received on, and wherein the information on the received beacon or probe response includes at least a service set identifier in the beacon or probe response.

35. (New) A method as recited in claim 18, wherein the management entity also manages any client stations of the managed APs, and wherein the receiving a scan request also includes a request to request any associated clients to listen for beacons or probe responses, the method further comprising:

sending a client request to one or more client stations associated with the AP to listen for beacons and probe responses; and

in the case that a client request was sent, receiving a client report at the AP from at least one of the client stations to which the client request was sent, the

client report including information on any beacon or probe response received from a potential rogue AP.

36. (New) A computer-readable medium as recited in claim 26, wherein the information stored in the AP database on each managed AP includes a maximum power setting or a frequency setting or both a maximum power and a frequency setting.

37. (New) A computer-readable medium as recited in claim 26, wherein the detection information includes at least the channel the detected AP's beacon or probe response was received on, and wherein the information on the received beacon or probe response includes at least a service set identifier in the beacon or probe response.

38. (New) A computer-readable medium as recited in claim 26, wherein the sending a scan request to one or more managed APs of the wireless network includes a request for the receiving managed AP to request the AP's clients to scan for beacons and probe responses.